

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-66986

(P2001-66986A)

(43) 公開日 平成13年3月16日 (2001.3.16)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-マ-ト*(参考)
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 B 5 B 0 4 9
G 0 6 F 17/60		G 0 6 F 15/21	Z 5 J 1 0 4
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B 5 K 0 3 2
9/32			6 7 5 A 5 K 0 3 4
12/40		11/00	3 2 0 9 A 0 0 1
審査請求 未請求 請求項の数11 O L (全 17 頁) 最終頁に続く			

(21) 出願番号 特願平11-239205

(22) 出願日 平成11年8月26日 (1999.8.26)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 石黒 隆二

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 海老原 宗毅

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

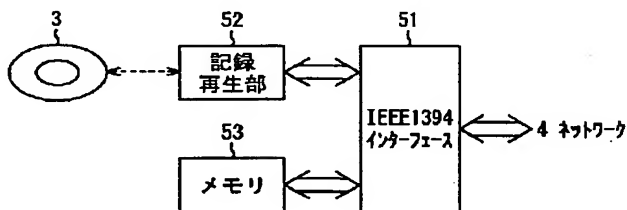
最終頁に続く

(54) 【発明の名称】 送信装置および方法、受信装置および方法、通信システム、並びにプログラム格納媒体

## (57) 【要約】

【課題】 不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限する。

【解決手段】 メモリ53は、コンテンツ管理データのハッシュ値を記憶する。IEEE1394インターフェース51は、ネットワークを介して接続されているパーソナルコンピュータを認証するとき、パーソナルコンピュータにコンテンツ管理データを送信するとともに、パーソナルコンピュータからコンテンツ管理データのハッシュ値を受信する。IEEE1394インターフェース51は、パーソナルコンピュータを認証するとき、受信したコンテンツ管理データのハッシュ値と、記憶しているコンテンツ管理データのハッシュ値との一致を判定する。



DVDドライブ 2

**【特許請求の範囲】**

**【請求項1】** 第1のデータおよび前記第1のデータの利用の制限を記述する第2のデータが記録されている記録媒体を駆動して、前記第1のデータを受信装置に送信する送信装置において、

前記第2のデータの暗号値を記憶する記憶手段と、  
前記受信装置を認証する場合、前記受信装置に前記第2のデータを送信するとともに、前記受信装置から前記第2のデータの暗号値を受信する通信手段と、  
前記受信装置を認証する場合、前記通信手段が受信した前記第2のデータの暗号値と、前記記憶手段が記憶している前記第2のデータの暗号値との一致を判定する判定手段とを含むことを特徴とする送信装置。

**【請求項2】** 前記記憶手段は、認証以外の処理において、前記第2のデータの暗号値の書き込みまたは読み出しを禁止することを特徴とする請求項1に記載の送信装置。

**【請求項3】** 前記記憶手段は、耐タンパー性を有することを特徴とする請求項1に記載の送信装置。

**【請求項4】** 第1のデータおよび前記第1のデータの利用の制限を記述する第2のデータが記録されている記録媒体を駆動して、前記第1のデータを受信装置に送信する送信装置の送信方法において、  
前記第2のデータの暗号値を記憶する記憶ステップと、  
前記受信装置を認証する場合、前記受信装置に前記第2のデータを送信するとともに、前記受信装置から前記第2のデータの暗号値を受信する通信ステップと、  
前記受信装置を認証する場合、前記通信ステップの処理で受信した前記第2のデータの暗号値と、前記記憶ステップの処理で記憶している前記第2のデータの暗号値との一致を判定する判定ステップとを含むことを特徴とする送信方法。

**【請求項5】** 第1のデータおよび前記第1のデータの利用の制限を記述する第2のデータが記録されている記録媒体を駆動して、前記第1のデータを受信装置に送信する送信処理用のプログラムであって、  
前記第2のデータの暗号値を記憶する記憶ステップと、  
前記受信装置を認証する場合、前記受信装置に前記第2のデータを送信するとともに、前記受信装置から前記第2のデータの暗号値を受信する通信ステップと、  
前記受信装置を認証する場合、前記通信ステップの処理で受信した前記第2のデータの暗号値と、前記記憶ステップの処理で記憶している前記第2のデータの暗号値との一致を判定する判定ステップとからなることを特徴とするプログラムを送信装置に実行させるプログラム格納媒体。

**【請求項6】** 送信装置が送信した第1のデータを受信する受信装置において、  
前記送信装置を認証する場合、前記送信装置から第1のデータの利用の制限を記述する第2のデータを受信する

とともに、前記送信装置に前記第2のデータの暗号値を送信する通信手段と、

前記送信装置を認証する場合、前記通信手段が受信した第2のデータを基に、前記第2のデータの暗号値を生成する暗号値生成手段とを含むことを特徴とする受信装置。

**【請求項7】** 所定のビット数の乱数を生成する乱数生成手段を更に含み、前記通信手段は、前記送信装置に、前記乱数生成手段が生成した前記乱数とともに、前記第2のデータの暗号値を送信することを特徴とする請求項6に記載の受信装置。

**【請求項8】** 前記通信手段が受信した前記第2のデータを基に、前記第1のデータの受信後の前記第1のデータの利用の制限を記述する第3のデータを生成する利用制限データ生成手段を更に含み、  
前記暗号値生成手段は、前記利用制限データ生成手段が生成した前記第3のデータの暗号値を更に生成し、  
前記通信手段は、前記送信装置に、前記第3のデータの暗号値とともに、前記第2のデータの暗号値を送信することを特徴とする請求項6に記載の受信装置。

**【請求項9】** 送信装置が送信した第1のデータを受信する受信装置の受信方法において、  
前記送信装置を認証する場合、前記送信装置から第1のデータの利用の制限を記述する第2のデータを受信するとともに、前記送信装置に前記第2のデータの暗号値を送信する通信ステップと、  
前記送信装置を認証する場合、前記通信ステップの処理で受信した第2のデータを基に、前記第2のデータの暗号値を生成する暗号値生成ステップとを含むことを特徴とする受信方法。

**【請求項10】** 送信装置が送信した第1のデータを受信する受信処理用のプログラムであって、  
前記送信装置を認証する場合、前記送信装置から第1のデータの利用の制限を記述する第2のデータを受信するとともに、前記送信装置に前記第2のデータの暗号値を送信する通信ステップと、  
前記送信装置を認証する場合、前記通信ステップの処理で受信した第2のデータを基に、前記第2のデータの暗号値を生成する暗号値生成ステップとからなることを特徴とするプログラムを受信装置に実行させるプログラム格納媒体。

**【請求項11】** 第1のデータおよび前記第1のデータの利用の制限を記述する第2のデータが記録されている記録媒体を駆動して、前記第1のデータを送信する送信装置、および前記第1のデータを受信する受信装置からなる通信システムにおいて、

前記送信装置は、  
前記第2のデータの暗号値を記憶する記憶手段と、  
前記受信装置を認証する場合、前記受信装置に前記第2のデータを送信するとともに、前記受信装置から前記第

2のデータの暗号値を受信する第1の通信手段と、前記受信装置を認証する場合、前記第1の通信手段が受信した前記第2のデータの暗号値と、前記記憶手段が記憶している前記第2のデータの暗号値との一致を判定する判定手段とを含み、

前記受信装置は、

前記送信装置を認証する場合、前記送信装置から前記第2のデータを受信するとともに、前記送信装置に前記第2のデータの暗号値を送信する第2の通信手段と、

前記送信装置を認証する場合、前記第2の通信手段が受信した第2のデータを基に、前記第2のデータの暗号値を生成する暗号値生成手段とを含むことを特徴とする通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、送信装置および方法、受信装置および方法、通信システム、並びにプログラム格納媒体に関し、特に、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようにした送信装置および方法、受信装置および方法、通信システム、並びにプログラム格納媒体に関する。

【0002】

【従来の技術】画像または音声などのコンテンツデータ、またはコンピュータプログラムなどを使用者者に提供する提供者は、これらのコンテンツデータなどが無制限にコピーされて利用されることを防止するため、これらのコンテンツデータなどを予め暗号化して使用者に提供することができる。

【0003】このような場合において、所定の暗号鍵を有する正当な使用者だけが、暗号化されているコンテンツデータなどを利用できる。

【0004】また、コンテンツデータなどの不正な利用を、より強力に防止するため、一部の装置は、コンテンツデータなどを再生する装置とコンテンツデータなどを記録している記録媒体を駆動する装置とを相互認証させるなどの方法が採用する。

【0005】更に、提供者がコンテンツデータなどの利用の回数を制限したいとき、提供者は、コンテンツデータなどとともにコンテンツデータなどの利用の回数を管理するためのデータを記録媒体に記録して、提供する場合がある。この場合、記録媒体を駆動する装置は、記録媒体に記録されているコンテンツデータなどを読み出すとき、コンテンツデータなどの利用の回数を管理するためのデータを基に、コンテンツデータなどを読み出す回数が予め設定されている回数を越えるか否かを判定して、コンテンツデータなどを読み出す回数が予め設定されている回数を越えたとき、コンテンツデータなどの利用を禁止する。

【0006】

【発明が解決しようとする課題】しかしながら、コンテンツデータなどと共に、利用の回数を管理するためのデータを他の記録媒体にバックアップして、そのコンテンツデータなどを利用した後、バックアップされた利用の回数を管理するためのデータを元の記録媒体に戻せば、利用者は、無制限にコンテンツデータなどを利用することができる。

【0007】同様に、そのコンテンツデータなどを他の記録媒体に移動するとき、予め、コンテンツデータなどと共に、利用の回数を管理するためのデータを更に他の記録媒体にバックアップして、そのコンテンツデータなどを他の記録媒体に移動した後、更に他の記録媒体からコンテンツデータなどと共に、利用の回数を管理するためのデータを元の記録媒体に戻せば、利用者は、無制限にコンテンツデータなどを複製することができる。

【0008】コンテンツデータなどの他の記録媒体への移動の処理における、コンテンツデータなどまたは利用の回数を管理するためのデータの削除の処理を妨害しても、同様に、無制限なコンテンツデータなどの複製が可能になり、利用者は、無制限にコンテンツデータなどを利用することができる。

【0009】本発明はこのような状況に鑑みてなされたものであり、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようにすることを目的とする。

【0010】

【課題を解決するための手段】請求項1に記載の送信装置は、第2のデータの暗号値を記憶する記憶手段と、受信装置を認証する場合、受信装置に第2のデータを送信するとともに、受信装置から第2のデータの暗号値を受信する通信手段と、受信装置を認証する場合、通信手段が受信した第2のデータの暗号値と、記憶手段が記憶している第2のデータの暗号値との一致を判定する判定手段とを含むことを特徴とする。

【0011】記憶手段は、認証以外の処理において、第2のデータの暗号値の書き込みまたは読み出しを禁止するようにすることができる。

【0012】記憶手段は、耐タンパー性を有するようにすることができる。

【0013】請求項4に記載の送信方法は、第2のデータの暗号値を記憶する記憶ステップと、受信装置を認証する場合、受信装置に第2のデータを送信するとともに、受信装置から第2のデータの暗号値を受信する通信ステップと、受信装置を認証する場合、通信ステップの処理で受信した第2のデータの暗号値と、記憶ステップの処理で記憶している第2のデータの暗号値との一致を判定する判定ステップとを含むことを特徴とする。

【0014】請求項5に記載のプログラム格納媒体のプログラムは、第2のデータの暗号値の記憶を制御する記憶制御ステップと、受信装置を認証する場合、受信装置

に第2のデータを送信するとともに、受信装置から第2のデータの暗号値を受信する通信ステップと、受信装置を認証する場合、通信ステップの処理で受信した第2のデータの暗号値と、記憶制御ステップの処理で記憶している第2のデータの暗号値との一致を判定する判定ステップとを含むことを特徴とする。

【0015】請求項6に記載の受信装置は、送信装置を認証する場合、送信装置から第1のデータの利用の制限を記述する第2のデータを受信するとともに、送信装置に第2のデータの暗号値を送信する通信手段と、送信装置を認証する場合、通信手段が受信した第2のデータを基に、第2のデータの暗号値を生成する暗号値生成手段とを含むことを特徴とする。

【0016】受信装置は、所定のビット数の乱数を生成する乱数生成手段を更に設け、通信手段は、送信装置に、乱数生成手段が生成した乱数とともに、第2のデータの暗号値を送信するようにすることができる。

【0017】受信装置は、通信手段が受信した第2のデータを基に、第1のデータの受信後の第1のデータの利用の制限を記述する第3のデータを生成する利用制限データ生成手段を更に設け、暗号値生成手段は、利用制限データ生成手段が生成した第3のデータの暗号値を更に生成し、通信手段は、送信装置に、第3のデータの暗号値とともに、第2のデータの暗号値を送信するようにすることができる。

【0018】請求項9に記載の受信方法は、送信装置を認証する場合、送信装置から第1のデータの利用の制限を記述する第2のデータを受信するとともに、送信装置に第2のデータの暗号値を送信する通信ステップと、送信装置を認証する場合、通信ステップの処理で受信した第2のデータを基に、第2のデータの暗号値を生成する暗号値生成ステップとを含むことを特徴とする。

【0019】請求項10に記載のプログラム格納媒体のプログラムは、送信装置を認証する場合、送信装置から第1のデータの利用の制限を記述する第2のデータを受信するとともに、送信装置に第2のデータの暗号値を送信する通信ステップと、送信装置を認証する場合、通信ステップの処理で受信した第2のデータを基に、第2のデータの暗号値を生成する暗号値生成ステップとを含むことを特徴とする。

【0020】請求項11に記載の通信システムは、送信装置が、第2のデータの暗号値を記憶する記憶手段と、受信装置を認証する場合、受信装置に第2のデータを送信するとともに、受信装置から第2のデータの暗号値を受信する第1の通信手段と、受信装置を認証する場合、第1の通信手段が受信した第2のデータの暗号値と、記憶手段が記憶している第2のデータの暗号値との一致を判定する判定手段とを含み、受信装置が、送信装置を認証する場合、送信装置から第2のデータを受信するとともに、送信装置に第2のデータの暗号値を送信する第2

の通信手段と、送信装置を認証する場合、第2の通信手段が受信した第2のデータを基に、第2のデータの暗号値を生成する暗号値生成手段とを含むことを特徴とする。

【0021】請求項1に記載の送信装置、請求項4に記載の送信方法、および請求項5に記載のプログラム格納媒体においては、第2のデータの暗号値が記憶され、受信装置を認証する場合、受信装置に第2のデータが送信されるとともに、受信装置から第2のデータの暗号値が受信され、受信装置を認証する場合、受信した第2のデータの暗号値と、記憶している第2のデータの暗号値との一致が判定される。

【0022】請求項6に記載の受信装置、請求項9に記載の受信方法、および請求項10に記載のプログラム格納媒体においては、送信装置を認証する場合、送信装置から第1のデータの利用の制限を記述する第2のデータが受信されるとともに、送信装置に第2のデータの暗号値が送信され、送信装置を認証する場合、受信した第2のデータを基に、第2のデータの暗号値が生成される。

【0023】請求項11に記載の通信システムにおいては、第2のデータの暗号値が記憶され、受信装置を認証する場合、受信装置に第2のデータが送信されるとともに、受信装置から第2のデータの暗号値が受信され、受信装置を認証する場合、受信した第2のデータの暗号値と記憶している第2のデータの暗号値との一致が判定され、送信装置を認証する場合、送信装置から第2のデータが受信されるとともに、送信装置に第2のデータの暗号値が送信され、送信装置を認証する場合、受信した第2のデータを基に、第2のデータの暗号値が生成される。

【0024】

【発明の実施の形態】図1は、本発明に係る記録システムの一実施の形態を示す図である。パーソナルコンピュータ1は、IEEE (Institute of Electrical and Electronic Engineers) 1394の規格に基づくネットワーク4を介して、DVD (Digital Versatile Disc) ドライブ2に接続されている。

【0025】パーソナルコンピュータ1は、DVDドライブ2からの音声または画像（動画または静止画像）などのデータであるコンテンツデータの供給に先立ち、DVDドライブ2と相互認証する。この相互認証の手続きにおいて、パーソナルコンピュータ1は、ネットワーク4を介して、DVDドライブ2より供給された、コンテンツデータの利用の条件等が記述されているコンテンツ管理データを受信する。パーソナルコンピュータ1は、パーソナルコンピュータ1でのコンテンツデータの利用（コンテンツの再生、またはコンテンツデータのコピーなど）に対応して、コンテンツ管理データを更新する。

【0026】パーソナルコンピュータ1は、DVDドライブ2より受信したコンテンツ管理データおよび更新した

コンテンツ管理データのそれぞれに、MD (Message Digest) 5 などの一方向ハッシュ関数を適用して、受信したコンテンツ管理データおよび更新したコンテンツ管理データのそれぞれの一方向性暗号値であるハッシュ値を求める。

【0027】受信したコンテンツ管理データのハッシュ値および更新したコンテンツ管理データのハッシュ値は、パーソナルコンピュータ1が生成した乱数と共に、DVDドライブ2に送信される。

【0028】パーソナルコンピュータ1は、DVDドライブ2と相互認証した後、例えば、DVDドライブ2から供給された音声または画像などのデータであるコンテンツデータ (暗号化されている) およびコンテンツデータを暗号化しているコンテンツ鍵を受信して、コンテンツ鍵でコンテンツデータを復号して、復号したコンテンツデータを再生する。

【0029】DVDドライブ2は、相互認証の手続きにおいて、DVD3に記録されているコンテンツ管理データを読み出して、ネットワーク4を介して、パーソナルコンピュータ1に送信する。DVDドライブ2は、相互認証の手続きにおいて、パーソナルコンピュータ1から、コンテンツ管理データのハッシュ値、更新されたコンテンツ管理データのハッシュ値、およびパーソナルコンピュータ1が生成した乱数を受信する。

【0030】DVDドライブ2は、パーソナルコンピュータ1と相互認証した後、装着されているDVD3に記録されている音声または画像などのデータであるコンテンツデータおよびコンテンツ鍵を読み出し、ネットワーク4を介して、パーソナルコンピュータ1に供給する。

【0031】DVDドライブ2は、後述するメモリに、DVD3に記録されているコンテンツ鍵を暗号化している暗号鍵である保存鍵、およびコンテンツ管理データにハッシュ関数を適用して得られた値であるハッシュ値を記憶している。

【0032】DVD3は、コンテンツ鍵で暗号化されているコンテンツデータ、コンテンツデータを暗号化している暗号鍵であるコンテンツ鍵、およびコンテンツデータの利用を管理するためのコンテンツ管理データを記録している。

【0033】DVD3に記録されているコンテンツデータは、共通鍵暗号方式であるDES (Data Encryption Standard) またはIDEA (International Data Encryption Algorithm) などの方式で、コンテンツ鍵で暗号化されている。

【0034】DVD3に記録されているコンテンツデータは、コンテンツ管理データに基づき、再生の回数、他の記録媒体へのコピー、他の記録媒体への移動が管理され、これらの操作が許可される。

【0035】コンテンツ管理データは、例えば、コンテンツデータが許可されている利用の形態 (例えば、コン

テンツの再生、コンテンツデータのコピー、またはコンテンツデータの移動など) を示すデータ、またはコンテンツの再生若しくはコンテンツデータのコピーの回数のデータなどから構成されている。コンテンツデータが利用されると、その利用の形態に対応して、コンテンツ管理データの値は変化する。

【0036】コンテンツ鍵は、DVDドライブ2のメモリに記憶されている保存鍵で暗号化されている。

【0037】ネットワーク4は、IEEE1394の規格に基づき、パーソナルコンピュータ1が出力したデータをDVDドライブ2に供給するとともに、DVDドライブ2が出力したデータをパーソナルコンピュータ1に供給する。

【0038】図2は、パーソナルコンピュータ1の構成を説明するブロック図である。CPU (Central Processing Unit) 21は、各種アプリケーションプログラムや、OS (Operating System)を実際に実行する。ROM (Read-only Memory) 22は、一般的には、CPU21が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random Access Memory) 23は、CPU21の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスまたはメモリバスなどから構成されるホストバス24により相互に接続されている。

【0039】ホストバス24は、ブリッジ25を介して、PCI (Peripheral Component Interconnect/Interface)バスなどの外部バス26に接続されている。

【0040】キーボード28は、CPU21に各種の指令を入力するとき、ユーザにより操作される。マウス29は、モニタ30の画面上のポイントの指示や選択を行うとき、ユーザにより操作される。モニタ30は、液晶表示装置またはCRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。HDD (Hard Disk Drive) 31およびFDD (Floppy Disk Drive) 32は、それぞれハードディスクまたはフロッピーディスクを駆動し、それらにCPU21によって実行するプログラムや情報を記録または再生させる。これらのキーボード28乃至FDD32は、インターフェース27に接続されており、インターフェース27は、外部バス26、ブリッジ25、およびホストバス24を介してCPU21に接続されている。

【0041】IEEE1394インターフェースボード33は、ネットワーク4が接続され、CPU21、またはHDD31から供給されたデータを、IEEE1394に規定されている方式のパケットに格納して、ネットワーク4を介して、送信するとともに、ネットワーク4を介して、受信したパケットに格納されているデータをCPU21、またはHDD31に出力する。IEEE1394インターフェースボード33は、また、IEEE1394の規定に基づく所定の処理を実行する。

【0042】IEEE1394インターフェースボード33は、外部バス26、ブリッジ25、およびホストバス24を介してCPU21に接続されている。

【0043】次に、図3のブロック図を参照して、DVDドライブ2の構成を説明する。IEEE1394インターフェース51は、ネットワーク4が接続され、記録再生部52またはメモリ53から供給されたデータを、IEEE1394に規定されている方式のパケットに格納して、ネットワーク4を介して、パーソナルコンピュータ1に送信するとともに、ネットワーク4を介して、パーソナルコンピュータ1から受信したパケットに格納されているデータを記録再生部52またはメモリ53に出力する。IEEE1394インターフェース51は、また、IEEE1394の規定に基づく所定の処理を実行する。

【0044】IEEE1394インターフェース51は、また、パーソナルコンピュータ1と、後述する相互認証の処理を実行する。IEEE1394インターフェース51は、相互認証の処理のときのみ、メモリ53に記憶されているデータを読み出すとともに、メモリ53に所定のデータを記憶させる。

【0045】メモリ53は、物理的に分解されたときに内部の構造をわかりにくくするためのアルミニウムの層を有し、DVDドライブ2から取り外されたとき、単独で動作させにくくする為に、所定の限られた範囲の電圧でのみ動作するなど耐タンパ性を有する半導体メモリで、保存鍵およびコンテンツ管理データのハッシュ値を記憶している。

【0046】記録再生部52は、DVD3が装着され、装着されているDVD3に記録されているコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを読み出してIEEE1394インターフェース51に出力するとともに、装着されているDVD3にIEEE1394インターフェース51から供給されたコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを記録させる。

【0047】図4は、DVDドライブ2に記憶されているデータ、またはDVD3に記録されているデータを説明する図である。DVD3は、保存鍵により暗号化されているコンテンツ鍵、コンテンツ鍵により暗号化されているコンテンツデータ、およびコンテンツデータの利用の形態を管理するためのコンテンツ管理データが記録されている。

【0048】DVDドライブ2のメモリ53は、保存鍵、およびコンテンツ管理データに所定のハッシュ関数を適用して得られたハッシュ値を記憶している。DVDドライブ2のメモリ53に記憶されている保存鍵、またはコンテンツ管理データのハッシュ値は、IEEE1394インターフェース51がパーソナルコンピュータ1と相互認証するときのみ、メモリ53から読み出され、または値が更新される。

【0049】図5は、DVDドライブ2およびパーソナル

コンピュータ1が相互認証するとき、ネットワーク4を介して、伝送されるデータの一部を説明する図である。コンテンツデータの利用に伴う相互認証において、パーソナルコンピュータ1は、所定のビット数の乱数（例えば、64ビット）を生成するとともに、DVDドライブ2から受信した現在のコンテンツ管理データに対して、コンテンツデータの利用に対応する変更を加えて更新し、更新後のコンテンツ管理データを生成する。

【0050】パーソナルコンピュータ1は、DVDドライブ2から受信したコンテンツ管理データおよび更新したコンテンツ管理データのそれぞれに、MD5などの一方方向ハッシュ関数を適用して、受信したコンテンツ管理データおよび更新したコンテンツ管理データのそれぞれの一方方向性暗号値であるハッシュ値を求める。

【0051】パーソナルコンピュータ1は、生成した乱数、現在のコンテンツ管理データのハッシュ値、および更新後のコンテンツ管理データのハッシュ値を、DVDドライブ2に送信する。

【0052】パーソナルコンピュータ1が生成した乱数、現在のコンテンツ管理データのハッシュ値、およびパーソナルコンピュータ1が更新したコンテンツ管理データのハッシュ値を受信したDVDドライブ2は、パーソナルコンピュータ1が生成した乱数、現在のコンテンツ管理データ、および更新されたコンテンツ管理データのそれぞれを暗号化する。

【0053】DVDドライブ2は、暗号化したパーソナルコンピュータ1が生成した乱数、暗号化した現在のコンテンツ管理データのハッシュ値、および暗号化した更新されたコンテンツ管理データのハッシュ値を、パーソナルコンピュータ1に送信する。

【0054】DVDドライブ2は、所定のビット数の乱数（例えば、64ビット）を生成して、パーソナルコンピュータ1に送信する。

【0055】パーソナルコンピュータ1は、DVDドライブ2から送信された所定のビット数の乱数を暗号化して、DVDドライブ2に送信する。

【0056】次に、本発明に係る記録システムのコンテンツの再生の処理を、図6のフローチャートを参照して説明する。ステップS11において、パーソナルコンピュータ1およびDVDドライブ2は、相互認証して、共通鍵を生成する。相互認証の処理の詳細は、図7のフローチャートを参照して後述する。ステップS12において、DVDドライブ2のIEEE1394インターフェース51は、メモリ53に記憶されている保存鍵を読み出し、記録再生部52に、装着されているDVD3からコンテンツ鍵を読み出させる。メモリ53に記憶されている保存鍵を読み出す処理は、ステップS11の相互認証の処理で実行してもよい。DVDドライブ2のIEEE1394インターフェース51は、コンテンツ鍵を保存鍵で復号する。

【0057】ステップS13において、DVDドライブ2



のIEEE1394インターフェース51は、ステップS11で生成された共通鍵で、コンテンツ鍵を暗号化する。ステップS14において、DVDドライブ2のIEEE1394インターフェース51は、ネットワーク4を介して、共通鍵で暗号化されたコンテンツ鍵をパーソナルコンピュータ1に送信する。

【0058】ステップS15において、パーソナルコンピュータ1のIEEE1394インターフェースボード33は、ネットワーク4を介して、DVDドライブ2から送信された、共通鍵で暗号化されたコンテンツ鍵を受信する。ステップS16において、DVDドライブ2のIEEE1394インターフェース51は、記録再生部52に、装着されているDVD3から、コンテンツ鍵で暗号化されているコンテンツデータを読み出させる。DVDドライブ2のIEEE1394インターフェース51は、ネットワーク4を介して、コンテンツ鍵で暗号化されているコンテンツデータをパーソナルコンピュータ1に送信する。

【0059】ステップS17において、パーソナルコンピュータ1のIEEE1394インターフェースボード33は、DVDドライブ2から送信された、コンテンツ鍵で暗号化されているコンテンツデータを受信する。ステップS18において、パーソナルコンピュータ1のCPU21は、ステップS15で受信したコンテンツ鍵を、ステップS11で生成した共通鍵で復号する。

【0060】ステップS19は、パーソナルコンピュータ1のCPU21は、復号したコンテンツ鍵で、ステップS17で受信したコンテンツデータを復号する。

【0061】ステップS20において、パーソナルコンピュータ1のIEEE1394インターフェースボード33は、ステップS11の相互認証の処理で更新されたコンテンツ管理データを、ネットワーク4を介して、DVDドライブ2に送信する。ステップS21において、DVDドライブ2のIEEE1394インターフェース51は、更新されたコンテンツ管理データを、受信する。ステップS22において、DVDドライブ2の記録再生部52は、装着されているDVD3に更新されたコンテンツ管理データを記録させる。

【0062】ステップS23において、パーソナルコンピュータ1は、復号したコンテンツデータからコンテンツを再生して、処理は終了する。

【0063】このように、パーソナルコンピュータ1は、DVDドライブ2からコンテンツ鍵およびコンテンツデータを受信して、コンテンツを再生する。

【0064】次に、図6のフローチャートのステップS11の処理に対応する、パーソナルコンピュータ1およびDVDドライブ2の相互認証の処理を、図7のフローチャートを参照して説明する。ステップS31において、DVDドライブ2のIEEE1394インターフェース51は、記録再生部52に、装着されているDVD3からコンテンツ管理データを読み出させる。IEEE1394インターフェース

51は、ネットワーク4を介して、コンテンツ管理データをパーソナルコンピュータ1に送信する。

【0065】ステップS51において、パーソナルコンピュータ1のIEEE1394インターフェースボード33は、ネットワーク4を介して、DVDドライブ2から送信されたコンテンツ管理データを受信する。ステップS52において、パーソナルコンピュータ1のCPU21は、DVDドライブ2から受信したコンテンツ管理データにMD5などの一方向ハッシュ関数を適用して、コンテンツ管理データのハッシュ値Haを計算する。

【0066】ステップS53において、パーソナルコンピュータ1のCPU21は、コンテンツの再生に対応させて、コンテンツの再生後のコンテンツ管理データを計算する。ステップS54において、パーソナルコンピュータ1のCPU21は、コンテンツの再生後のコンテンツ管理データにMD5などのハッシュ関数を適用して、コンテンツの再生後のコンテンツ管理データのハッシュ値Hbを計算する。

【0067】ステップS55において、パーソナルコンピュータ1のCPU21は、例えば、64ビットの乱数Raを生成する。ステップS56において、パーソナルコンピュータ1のIEEE1394インターフェースボード33は、ネットワーク4を介して、DVDドライブ2に、乱数Ra、ハッシュ値Ha、およびハッシュ値Hbを送信する。

【0068】ステップS32において、DVDドライブ2のIEEE1394インターフェース51は、パーソナルコンピュータ1から送信された乱数Ra、ハッシュ値Ha、およびハッシュ値Hbを受信する。ステップS33において、DVDドライブ2のIEEE1394インターフェース51は、メモリ53に記憶されているコンテンツ管理データのハッシュ値と、ステップS32で受信したハッシュ値Haとが一致するか否かを判定し、メモリ53に記憶されているコンテンツ管理データのハッシュ値と、ステップS32で受信したハッシュ値Haとが一致しないと判定された場合、コンテンツ管理データに改竄があったので、相互認証しないで、処理は終了する。

【0069】ステップS33において、メモリ53に記憶されているコンテンツ管理データのハッシュ値と、ステップS32で受信したハッシュ値Haとが一致すると判定された場合、コンテンツ管理データに改竄がなかったので、ステップS34に進み、DVDドライブ2のIEEE1394インターフェース51は、ステップS32で受信した乱数Ra、ハッシュ値Ha、およびハッシュ値Hbを暗号化する。

【0070】ステップS35において、DVDドライブ2のIEEE1394インターフェース51は、ネットワーク4を介して、暗号化した乱数Ra、暗号化したハッシュ値Ha、および暗号化したハッシュ値Hbをパーソナルコンピュータ1に送信する。

【0071】ステップS57において、パーソナルコンピュータ1のCPU21は、乱数R<sub>a</sub>、ハッシュ値H<sub>a</sub>、およびハッシュ値H<sub>b</sub>を暗号化する。

【0072】パーソナルコンピュータ1およびDVDドライブ2が共に正当である場合、ステップS34におけるDVDドライブ2のIEEE1394インターフェース51の暗号化の方式および暗号鍵は、ステップS57におけるパーソナルコンピュータ1のCPU21の暗号化の方式および暗号鍵と、それぞれ同一であり、パーソナルコンピュータ1およびDVDドライブ2において、同一の暗号化した乱数R<sub>a</sub>、暗号化したハッシュ値H<sub>a</sub>、および暗号化したハッシュ値H<sub>b</sub>が得られる。

【0073】ステップS58において、パーソナルコンピュータ1のIEEE1394インターフェースボード33は、ネットワーク4を介して、DVDドライブ2から送信された暗号化された乱数R<sub>a</sub>、暗号化されたハッシュ値H<sub>a</sub>、および暗号化されたハッシュ値H<sub>b</sub>を受信する。ステップS59において、パーソナルコンピュータ1のCPU21は、ステップS57で暗号化した乱数R<sub>a</sub>、暗号化したハッシュ値H<sub>a</sub>、および暗号化したハッシュ値H<sub>b</sub>のそれぞれと、ステップS58で受信した暗号化された乱数R<sub>a</sub>、暗号化されたハッシュ値H<sub>a</sub>、および暗号化されたハッシュ値H<sub>b</sub>のそれぞれとを比較して一致するか否かを判定し、暗号化した乱数R<sub>a</sub>、暗号化したハッシュ値H<sub>a</sub>、および暗号化したハッシュ値H<sub>b</sub>のそれぞれと、受信した暗号化された乱数R<sub>a</sub>、暗号化されたハッシュ値H<sub>a</sub>、および暗号化されたハッシュ値H<sub>b</sub>のいずれかが一致しないと判定された場合、DVDドライブ2は正当ではないので、DVDドライブ2を認証せず、処理は終了する。

【0074】ステップS36において、DVDドライブ2のIEEE1394インターフェース51は、64ビットの乱数R<sub>b</sub>を生成する。ステップS37において、DVDドライブ2のIEEE1394インターフェース51は、ネットワーク4を介して、生成した乱数R<sub>b</sub>をパーソナルコンピュータ1に送信する。ステップS38において、DVDドライブ2のIEEE1394インターフェース51は、乱数R<sub>b</sub>を暗号化する。

【0075】ステップS59において、暗号化した乱数R<sub>a</sub>、ハッシュ値H<sub>a</sub>、およびハッシュ値H<sub>b</sub>のそれぞれと、受信した暗号化された乱数R<sub>a</sub>、ハッシュ値H<sub>a</sub>、およびハッシュ値H<sub>b</sub>それぞれとが一致すると判定された場合、DVDドライブ2は正当なので、ステップS60に進み、パーソナルコンピュータ1のIEEE1394インターフェースボード33は、ネットワーク4を介して、DVDドライブ2が送信した乱数R<sub>b</sub>を受信する。

【0076】ステップS61において、パーソナルコンピュータ1のCPU21は、ステップS60で受信した乱数R<sub>b</sub>を暗号化する。パーソナルコンピュータ1およびDVDドライブ2が正当である場合、ステップS38に

おけるDVDドライブ2のIEEE1394インターフェース51の暗号化の方式および暗号鍵は、ステップS61におけるパーソナルコンピュータ1のCPU21の暗号化の方式および暗号鍵と、それぞれ同一であるので、暗号化された乱数の値は同一となる。

【0077】ステップS62において、パーソナルコンピュータ1のIEEE1394インターフェースボード33は、ネットワーク4を介して、ステップS61で暗号化した乱数R<sub>b</sub>をDVDドライブ2に送信する。

【0078】ステップS39において、DVDドライブ2のIEEE1394インターフェース51は、ネットワーク4を介して、パーソナルコンピュータ1が送信した暗号化された乱数R<sub>b</sub>を受信する。ステップS40において、DVDドライブ2のIEEE1394インターフェース51は、ステップS38で暗号化した乱数R<sub>b</sub>とステップS39で受信した暗号化された乱数R<sub>b</sub>とが一致するか否かを判定し、ステップS38で暗号化した乱数R<sub>b</sub>とステップS39で受信した暗号化された乱数R<sub>b</sub>とが一致しないと判定された場合、パーソナルコンピュータ1が正当ではないので、パーソナルコンピュータ1を認証しないで、処理は終了する。

【0079】ステップS40において、ステップS38で暗号化した乱数R<sub>b</sub>とステップS39で受信した暗号化された乱数R<sub>b</sub>とが一致すると判定された場合、パーソナルコンピュータ1が正当なので、ステップS41に進み、DVDドライブ2のIEEE1394インターフェース51は、メモリ53に、ステップS32で受信したハッシュ値H<sub>b</sub>を記憶させる。

【0080】ステップS42において、DVDドライブ2のIEEE1394インターフェース51は、パーソナルコンピュータ1を認証したので、乱数R<sub>a</sub>および乱数R<sub>b</sub>から共通鍵を生成し、DVDドライブ2の処理は終了する。

【0081】ステップS63において、パーソナルコンピュータ1のCPU21は、DVDドライブ2を認証したので、乱数R<sub>a</sub>および乱数R<sub>b</sub>から共通鍵を生成し、パーソナルコンピュータ1の処理は終了する。

【0082】このように、DVDドライブ2は、コンテンツ管理データのハッシュ値をメモリ53に記憶して、相互認証の手続きで、パーソナルコンピュータ1が計算したハッシュ値と比較するので、コンテンツ管理データが改竄されたとき、パーソナルコンピュータ1を認証しない。

【0083】DVDドライブ2は、相互認証の手続きで、受信した新たなコンテンツ管理データのハッシュ値を耐タンパ性を有するメモリ53に記憶するので、新たなコンテンツ管理データのハッシュ値の改竄が防止される。

【0084】パーソナルコンピュータ1は、その都度生成した乱数とともに、コンテンツ管理データのハッシュ値をDVDドライブ2に送信するので、パーソナルコンピュータ1になりすました機器が、コンテンツ管理データ



のハッシュ値を受信して記憶し、相互認証しようとしても、相互認証は成功しない。

【0085】なお、コンテンツデータの再生の回数が制限されていない場合など、ステップS53で計算されるコンテンツの再生後のコンテンツ管理データは、ステップS51で受信したコンテンツ管理データと同一でもよい。

【0086】次に、記録媒体に記録されているコンテンツデータを不正なコピーを防止しつつ、他の記録媒体に移動させることができる、他の記録システムについて説明する。図8は、コンテンツデータを移動することができる、記録システムの他の実施の形態を示す図である。パーソナルコンピュータ101は、SCSI (Small Computer System Interface) を介して、MO (Magneto-Optical disk) ドライブ102およびハードディスク装置104に接続されている。

【0087】MOドライブ102は、装着されているMO103に記録されている音声または画像のデータであるコンテンツデータを読み出し、パーソナルコンピュータ101または、ハードディスク装置104に供給する。MOドライブ102は、後述するメモリに、MO103に記録されているコンテンツ鍵を暗号化する暗号鍵である保存鍵、およびコンテンツ管理データにMD5などの一方向ハッシュ関数を適用して得られた値であるハッシュ値を記憶している。

【0088】MO103は、暗号化されているコンテンツデータ、コンテンツデータを暗号化している暗号鍵であるコンテンツ鍵、およびコンテンツデータの利用を管理するためのコンテンツ管理データを記録している。

【0089】MO103に記録されているコンテンツデータは、共通鍵暗号方式であるDESまたはIDEAなどの方式で、コンテンツ鍵で暗号化されている。

【0090】MO103に記録されているコンテンツデータは、コンテンツ管理データに基づき、再生回数、他の記録媒体へのコピー、他の記録媒体への移動が管理され、これらの操作が許可される。

【0091】コンテンツ管理データは、コンテンツデータが許可されている利用の形態を示すデータ、またはコンテンツの再生若しくはコンテンツデータのコピーの回数のデータなどから構成されている。コンテンツデータが利用されると、その利用の形態に対応して、コンテンツ管理データの値は変化する。

【0092】コンテンツ鍵は、MOドライブ102のメモリに記憶されている保存鍵で暗号化されている。

【0093】ハードディスク装置104は、内蔵されているハードディスクドライブにパーソナルコンピュータ101またはMOドライブ102から供給されたデータを記録するとともに、記録されているデータをパーソナルコンピュータ101またはMOドライブ102に供給する。

【0094】図9は、パーソナルコンピュータ101の構成を説明するブロック図である。CPU121乃至FDD132のそれぞれは、それぞれ図2のCPU21乃至FDD32と同様であるので、その説明は省略する。

【0095】SCSIインターフェースボード133は、所定のSCSIケーブルが接続され、CPU21、RAM123、またはHDD31から供給されたデータを、MOドライブ102またはハードディスク装置104に送信するとともに、MOドライブ102またはハードディスク装置104から受信したデータをCPU21、RAM123、またはHDD31に出力する。

【0096】SCSIインターフェースボード133は、外部バス126、ブリッジ125、およびホストバス124を介してCPU121に接続されている。

【0097】次に、図10のブロック図を参照して、MOドライブ102の構成を説明する。SCSIインターフェース151は、SCSIケーブルが接続され、記録再生部152またはメモリ153から供給されたデータを、パーソナルコンピュータ101またはハードディスク装置104に送信するとともに、パーソナルコンピュータ101またはハードディスク装置104から受信したデータを記録再生部152またはメモリ153に出力する。

【0098】SCSIインターフェース151は、パーソナルコンピュータ101またはハードディスク装置104と、図7のフローチャートを参照して説明した相互認証の処理を実行する。SCSIインターフェース151は、相互認証の処理のときのみ、メモリ153に記憶されているデータを読み出すとともに、メモリ153に所定のデータを記憶させる。

【0099】メモリ153は、物理的に分解されたときに内部の構造をわかりにくくするためのアルミニウムの層を有し、MOドライブ102から取り外されたとき、単独で動作させるべくするための、所定の限られた範囲の電圧でのみ動作するなど耐タンパー性を有する半導体メモリで、保存鍵およびコンテンツ管理データのハッシュ値を記憶している。

【0100】記録再生部152は、MO102が装着され、装着されているMO102に記録されているコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを読み出してSCSIインターフェース151に出力するとともに、装着されているMO102にSCSIインターフェース151から供給されたコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを記録させる。

【0101】次に、図11のブロック図を参照して、ハードディスク装置104の構成を説明する。SCSIインターフェース161は、SCSIケーブルが接続され、ハードディスクドライブ162またはメモリ163から供給されたデータを、パーソナルコンピュータ101またはMOドライブ102に送信するとともに、パーソナルコン

ピュータ101またはMOドライブ102から受信したデータをハードディスクドライブ162またはメモリ163に出力する。

【0102】SCSIインターフェース161は、パーソナルコンピュータ101またはMOドライブ102と、図7のフローチャートを参照して説明した相互認証の処理を実行する。SCSIインターフェース161は、相互認証の処理のときのみ、メモリ163に記憶されているデータを読み出すとともに、メモリ163に所定のデータを記憶させる。

【0103】メモリ163は、物理的に分解されたときに内部の構造をわかりにくくするためのアルミニウムの層を有し、ハードディスク装置104から取り外されたとき、単独で動作させにくくする為、所定の限られた範囲の電圧でのみ動作するなど耐タンパ性を有する半導体メモリで、保存鍵およびコンテンツ管理データのハッシュ値を記憶している。

【0104】ハードディスクドライブ162は、内蔵されているハードディスクに記録されているコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを読み出してSCSIインターフェース161に出力するとともに、内蔵されているハードディスクにSCSIインターフェース161から供給されたコンテンツデータ、コンテンツ鍵、またはコンテンツ管理データなどを記録させる。

【0105】図12は、図8に示す記録システムの、MOドライブ102に装着されているMO103に記録されているコンテンツデータを、ハードディスクドライブ162に移動する処理を説明するフローチャートである。ステップS81において、MOドライブ102の記録再生部152は、MO103に記憶されているコンテンツ管理データを基に、移動後のコンテンツ管理データを計算する。記録再生部152は、計算した移動後のコンテンツ管理データをSCSIインターフェース151に供給する。

【0106】ステップS82において、MOドライブ102のSCSIインターフェース151およびパーソナルコンピュータ101のSCSIインターフェースボード133は、図7のフローチャートを参照して説明した処理と同様の手続きで、相互認証して、共通鍵K1を生成する。

【0107】ただし、ステップS31において、SCSIインターフェースボード133は、パーソナルコンピュータ101に現在のコンテンツ管理データおよび移動後のコンテンツ管理データを送信し、パーソナルコンピュータ101は、受信した現在のコンテンツ管理データおよび移動後のコンテンツ管理データを基に、ハッシュ値を計算する。

【0108】ステップS83において、MOドライブ102のSCSIインターフェース151は、ステップS82の相互認証と同時に、メモリ153に記憶されているコ

ンテンツ管理データをステップS81で計算した移動後の値に変更させる。

【0109】ステップS84において、MOドライブ102のSCSIインターフェース151は、記録再生部152にMO103からコンテンツ鍵を読み出させ、メモリ153に記憶されている保存鍵でコンテンツ鍵を復号する。

【0110】ステップS85において、MOドライブ102のSCSIインターフェース151は、復号されたコンテンツ鍵をステップS82で生成した共通鍵K1で暗号化する。ステップS86において、MOドライブ102のSCSIインターフェース151は、共通鍵K1で暗号化されたコンテンツ鍵を、パーソナルコンピュータ101に送信する。

【0111】ステップS87において、パーソナルコンピュータ101のSCSIインターフェースボード133は、MOドライブ102から送信された暗号化されているコンテンツ鍵を受信する。

【0112】ステップS88において、パーソナルコンピュータ101のCPU121は、ステップS87で受信したコンテンツ鍵を、ステップS82で生成した共通鍵K1で復号する。

【0113】ステップS89において、ハードディスク装置104のハードディスクドライブ162は、移動後のコンテンツ管理データ（相互認証の処理に利用される）を計算する。

【0114】ステップS90において、ハードディスク装置104のSCSIインターフェース161およびパーソナルコンピュータ101のSCSIインターフェースボード133は、図7のフローチャートを参照して説明した処理と同様の手続きで、相互認証して、共通鍵K2を生成する。ステップS90のパーソナルコンピュータ101とハードディスク装置104の相互認証の処理で、パーソナルコンピュータ101は、ハードディスク装置104にステップS81でMOドライブ102が計算した移動後のコンテンツ管理データを送信する。

【0115】ステップS91において、ハードディスク装置104のSCSIインターフェース161は、ステップS90の相互認証と同時に、メモリ163に記憶されているコンテンツ管理データを、ステップS90で受信した移動後のコンテンツ管理データに変更させる。

【0116】ステップS92において、パーソナルコンピュータ101のCPU121は、ステップS88で復号されたコンテンツ鍵を、共通鍵K2で暗号化する。ステップS93において、パーソナルコンピュータ101のSCSIインターフェースボード133は、共通鍵K2で暗号化されているコンテンツ鍵をハードディスク装置104に送信する。

【0117】ステップS94において、ハードディスク装置104のSCSIインターフェース161は、パーソナ

ルコンピュータ101から送信された、共通鍵K2で暗号化されているコンテンツ鍵を受信する。

【0118】ステップS95において、ハードディスク装置104のSCSIインターフェース161は、ステップS94で受信したコンテンツ鍵を共通鍵K2で復号する。

【0119】ステップS96において、MOドライブ102の記録再生部152は、装着されているMO103からコンテンツ鍵を削除する。

【0120】ステップS97において、ハードディスク装置104のSCSIインターフェース161は、ステップS95で復号されたコンテンツ鍵を、メモリ163に記憶している保存鍵で暗号化する。ステップS98において、ハードディスク装置104のハードディスクドライブ162は、暗号化されたコンテンツ鍵を記録する。

【0121】ステップS99において、MOドライブ102のSCSIインターフェース151は、記録再生部152にMO103からコンテンツデータを読み出させ、ハードディスク装置104にコンテンツデータを移動する。

【0122】このように、図8に示す記録システムにおいては、MO103に記録されているコンテンツデータをハードディスク装置104に移動する。MO103に記録されているコンテンツデータを他のMOディスクにバックアップしておき、MO103に記録されているコンテンツデータを利用した後、バックアップされたコンテンツデータが記録されているMOディスクを使用しようとしても、ステップS82の相互認証の処理で不正と判定されるので、バックアップしたコンテンツデータを使用することができない。

【0123】なお、コンテンツデータが記録される記録媒体は、DVD3、MO103、またはハードディスクとして説明したが、光ディスク、半導体メモリ、磁気テープ、または印刷物（例えば、2次元バーコードが印刷された印刷物）でもよい。

【0124】また、記録媒体に記録するコンテンツデータは、音声または画像（動画または静止画像）として説明したが、コンピュータプログラム、所定のサーバなどへのアクセス権を記述したデータ（ファイル）、または所定のサービスを利用するためのデータを記憶したチケットなどでもよい。

【0125】コンテンツを再生する装置は、パーソナルコンピュータ1またはパーソナルコンピュータ101として説明したが、パーソナルコンピュータ1またはパーソナルコンピュータ101に限らず、セットトップボックスなどの家庭電化製品、サーバ、またはDVDドライブなどのコンピュータ周辺装置などでもよい。

【0126】パーソナルコンピュータ1またはパーソナルコンピュータ101が実行するコンテンツの再生の処理、相互認証の処理などのプログラムを内部が解析しに

くいソフトウェアとすれば、コンテンツデータの不正使用に対する防御をより強力にすることができる。

【0127】パーソナルコンピュータ1、パーソナルコンピュータ101、DVDドライブ2、MOドライブ102、またはハードディスク装置104は、IEEE1394の規格に基づくネットワーク4またはSCSIケーブルを介してデータを送信するとともに、受信すると説明したが、他のネットワーク、他のデータ転送用のインターフェースなどでもよい。

【0128】例えば、半導体メモリが内蔵された、シリアル制御されるメモリカードは、コンテンツデータである、暗号化した音楽データを記憶している。音楽を再生するとき、メモリカードは、所定のパーソナルコンピュータのインターフェースに装着される。

【0129】音楽の再生の回数を制限するため、そのメモリカードに記憶されているコンテンツ管理データは、音楽の再生の回数に対応してデクリメントされる。コンテンツ管理データが“0”になったとき、メモリカードが装着されているパーソナルコンピュータは、メモリカードに記憶されている音楽データを利用しない（音楽を再生しない）。

【0130】メモリカードが装着されるインターフェースが、コンテンツ管理データのハッシュ値を記憶すれば、メモリカードに記憶されているコンテンツ管理データを他のメモリカードにバックアップしても、その後に、一度でもメモリカードに記憶されている音楽データが利用されれば、バックアップされた音楽データを再生することはできない。

【0131】例えば、メモリカードが装着されるインターフェースが相互認証の処理の際に出力する信号を監視して、その信号を記録し、またその信号を改竄しても、コンテンツ管理データのハッシュ値は、その都度生成された乱数とともに、送信されるので、相互認証を成功させることは、不可能である。

【0132】このように、コンテンツデータが記録される記録媒体の種類、信号が送信される方式、インターフェースの種類などに拘わらず、不正な複製を防止することができる。

【0133】なお、メモリ53、メモリ153、またはメモリ163は、コンテンツ管理データにハッシュ関数を適用して得られるハッシュ値を記憶するとして説明したが、ハッシュ値に限らず、DESなどの共通鍵暗号方式で暗号化したコンテンツ管理データを記憶してもよい。

【0134】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールす

ることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【0135】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図13に示すように、磁気ディスク351（フロッピディスクを含む）、光ディスク352（CD-ROM(CompactDisc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク353（MD(Mini-Disc)を含む）、若しくは半導体メモリ354などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM302や、記憶部308を構成するハードディスクなどにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じてルータ、モデムなどのインターフェースを介して、ローカルエリアネットワーク、インターネット、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【0136】なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0137】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0138】

【発明の効果】請求項1に記載の送信装置、請求項4に記載の送信方法、および請求項5に記載のプログラム格納媒体によれば、第2のデータの暗号値が記憶され、受信装置を認証する場合、受信装置に第2のデータが送信されるとともに、受信装置から第2のデータの暗号値が受信され、受信装置を認証する場合、受信した第2のデータの暗号値と、記憶している第2のデータの暗号値との一致が判定されるようにしたので、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようになる。

【0139】請求項6に記載の受信装置、請求項9に記載の受信方法、および請求項10に記載のプログラム格納媒体によれば、送信装置を認証する場合、送信装置から第1のデータの利用の制限を記述する第2のデータが受信されるとともに、送信装置に第2のデータの暗号値が送信され、送信装置を認証する場合、受信した第2のデータを基に、第2のデータの暗号値が生成されるようにしたので、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようになる。

【0140】請求項11に記載の通信システムによれば、第2のデータの暗号値が記憶され、受信装置を認証する場合、受信装置に第2のデータが送信されるととも

に、受信装置から第2のデータの暗号値が受信され、受信装置を認証する場合、受信した第2のデータの暗号値と、記憶している第2のデータの暗号値との一致が判定され、送信装置を認証する場合、送信装置から第2のデータが受信されるとともに、送信装置に第2のデータの暗号値が送信され、送信装置を認証する場合、受信した第2のデータを基に、第2のデータの暗号値が生成されるようにしたので、不正な複製を防止して、確実に、コンテンツデータなどの利用の回数を制限することができるようになる。

【図面の簡単な説明】

【図1】本発明に係る記録システムの一実施の形態を示す図である。

【図2】パーソナルコンピュータ1の構成を説明するブロック図である。

【図3】DVDドライブ2の構成を説明するブロック図である。

【図4】DVDドライブ2に記憶されているデータ、またはDVD3に記録されているデータを説明する図である。

【図5】DVDドライブ2およびパーソナルコンピュータ1が相互認証するとき、ネットワーク4を介して、送信されるデータの一部を説明する図である。

【図6】コンテンツの再生の処理を説明するフローチャートである。

【図7】相互認証の処理を説明するフローチャートである。

【図8】記録システムの他の実施の形態を示す図である。

【図9】パーソナルコンピュータ101の構成を説明するブロック図である。

【図10】MOドライブ102の構成を説明するブロック図である。

【図11】ハードディスク装置104の構成を説明するブロック図である。

【図12】コンテンツの移動の処理を説明するフローチャートである。

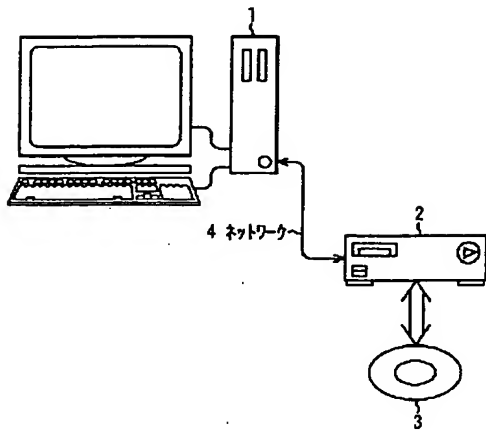
【図13】プログラム格納媒体を説明する図である。

【符号の説明】

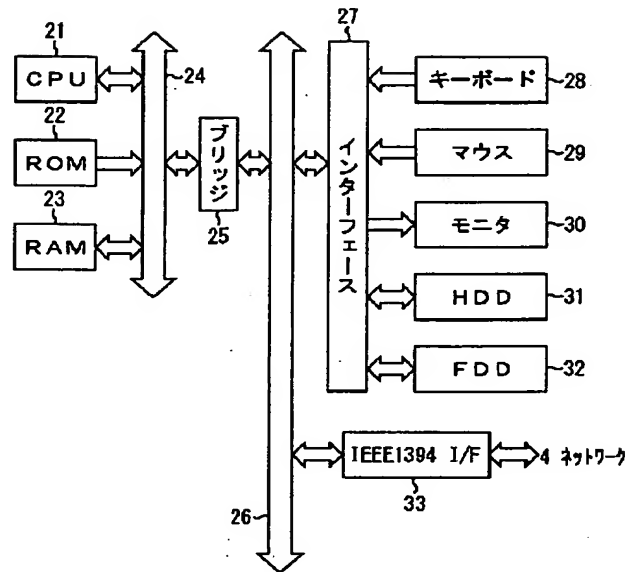
1 パーソナルコンピュータ, 2 DVDドライブ, 3 DVD, 4 ネットワーク, 21 CPU, 33 IEEE1394インターフェースボード, 51 IEEE1394インターフェース, 52 記録再生部, 53 メモリ, 101 パーソナルコンピュータ, 102 MOドライブ, 103 MO, 104 ハードディスク装置, 121 CPU, 133 SCSIインターフェースボード, 151 SCSIインターフェース, 152 記録再生部, 153 メモリ, 161 SCSIインターフェース, 162 ハードディスクドライブ, 163 メモリ, 301 CPU, 302 ROM, 303 RAM, 308 記憶部, 351 磁気デ

ディスク、 352 光ディスク、 353 光磁気ディスク、 354 半導体メモリ

【図1】

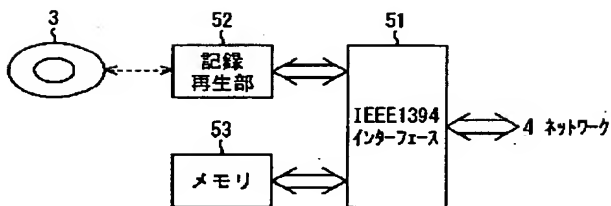


【図2】



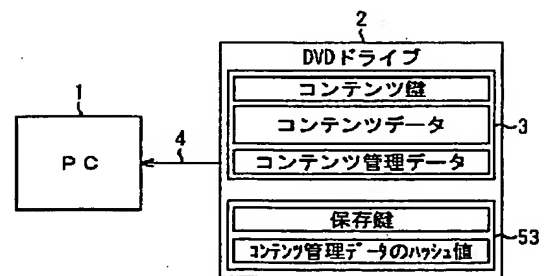
パーソナルコンピュータ 1

【図3】

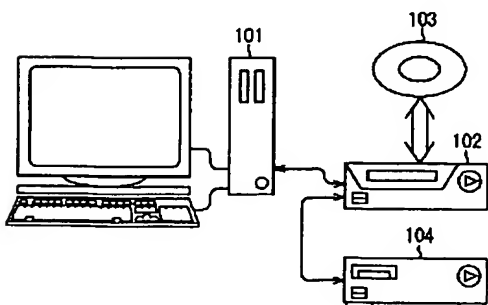


DVDドライブ 2

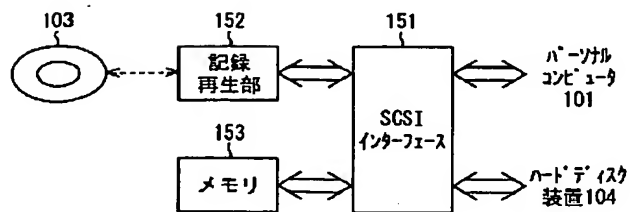
【図4】



【図8】

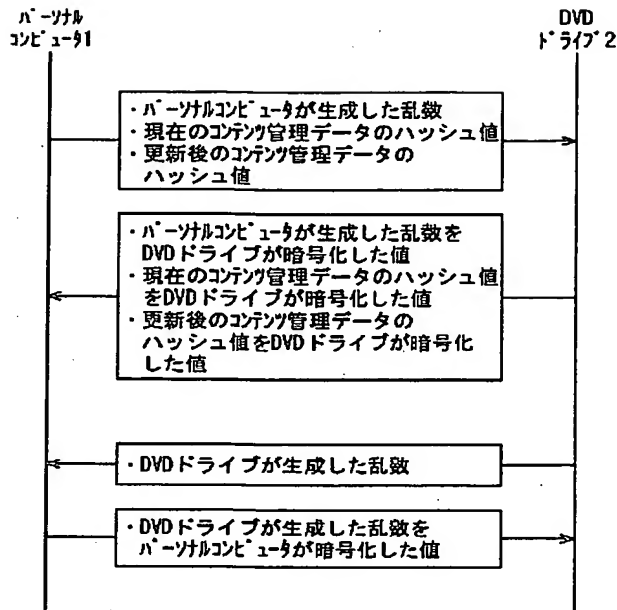


【図10】

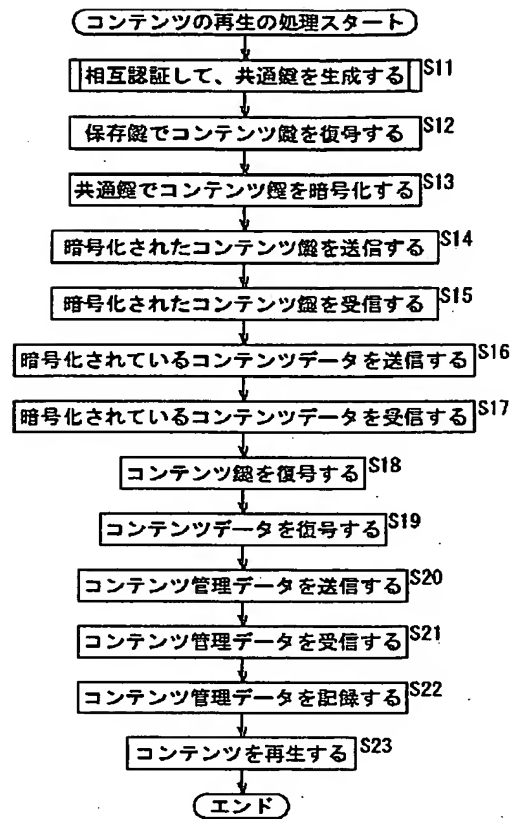


MOドライブ 102

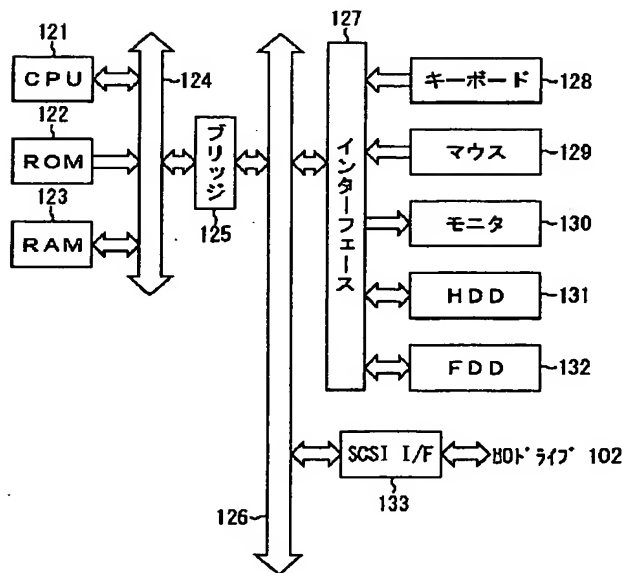
【図5】



【図6】

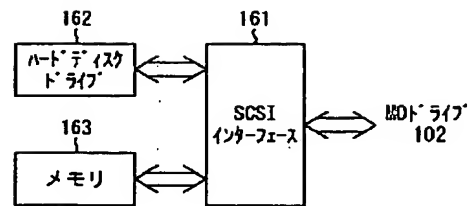


【図9】



パーソナルコンピュータ 101

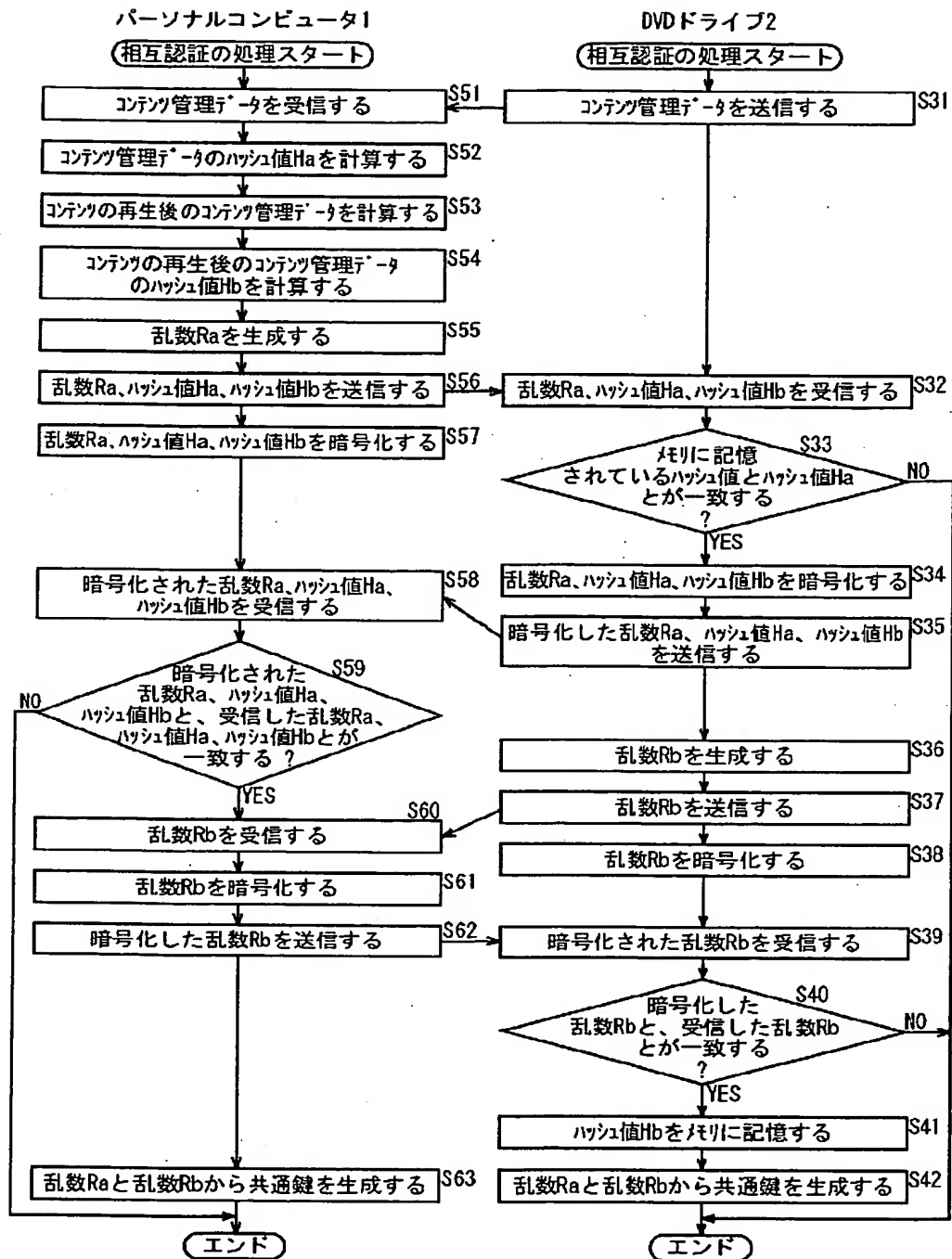
【図11】



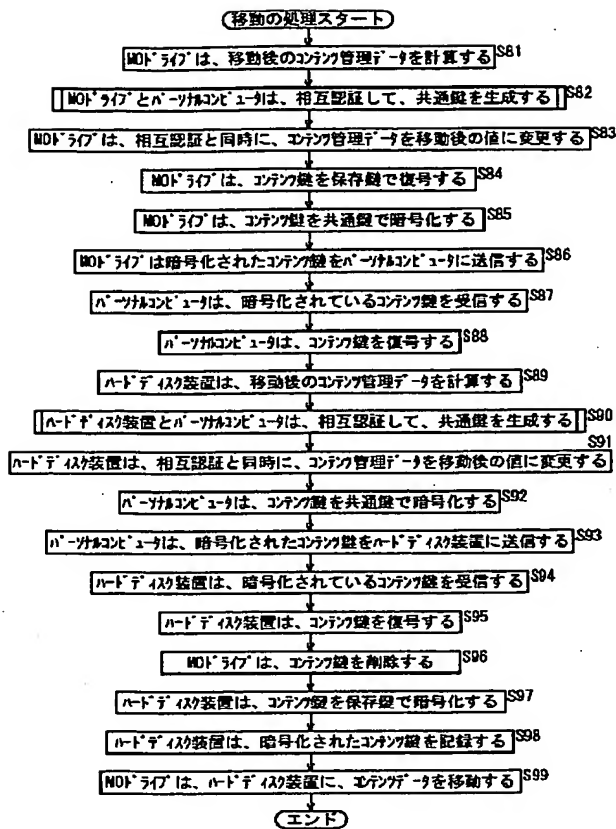
ハードディスク装置 104



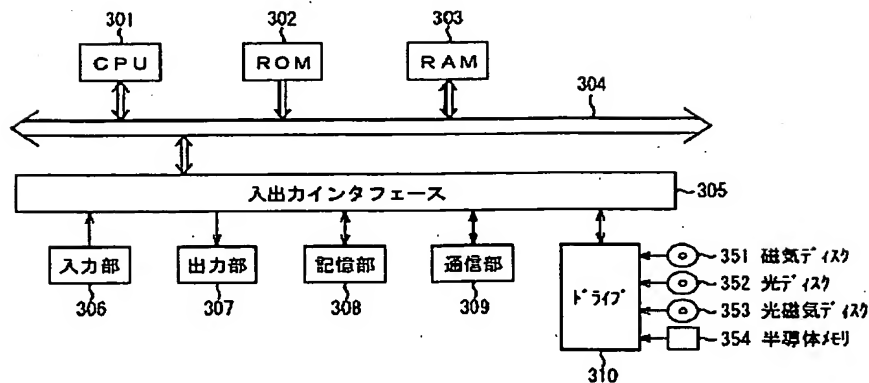
【図7】



【図12】



【図13】



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

テーマコード (参考)

H 0 4 L 29/10

H 0 4 L 13/00

3 0 9 C

Fターム (参考) 5B049 AA05 BB11 CC05 CC08 DD01  
DD05 EE03 FF03 FF04 FF09  
GG04 GG07 GG10  
5J104 AA13 FA07 JA01 KA06 NA02  
NA12 NA27 NA31 NA32 PA04  
PA07  
5K032 AA08 DB19  
5K034 BB03 DD02 HH01  
9A001 EE03 GG22 HH15 JJ19 KK43  
KK62 LL03

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**